Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application. As requested by the Examiner, this listing of the claims shows all amendments, and claims status, relative to the claims originally submitted by the applicant on March 3, 2006 for examination.

1. - 8. (Canceled).

9. - 16. (Canceled).

17. - 154. (Canceled).

155. **(Currently amended)** A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data pertaining to ~~at least one party~~ an actual recipient of e-mail in a data file ~~on a computer associated with said at least one party for purposes of retrieving e-mail~~, said stored ~~recipient~~ data file containing identifying data that identifies said ~~at least one party~~ actual e-mail recipient and further being associated with said actual recipient's email address;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to a recipient e-mail address;

d) detecting an access event, and discovering ~~the~~ said stored ~~recipient~~ data file that is associated with said actual recipient's e-mail address ~~that identifies the recipient associated with the recipient e-mail address to which such e-mail was delivered~~; and

e) ~~generating a confirmation of receipt notice wherein the discovered recipient data is included in said confirmation of receipt notice; and~~

- 2 -

f) sending <u>identifying data contained in said discovered data file for confirming proper delivery of said e-mail</u> ~~said confirmation of receipt notice, wherein the discovered recipient data contained in said confirmation of receipt notice can be compared to delivery information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient~~ .

156.   Canceled.

157.   (Currently amended)   The method as in claim 155, wherein said access event comprises access of said e-mail that was delivered to said <u>actual</u> recipient e-mail address.

158.   (Currently amended) The method as in claim 155, wherein said access event comprises access of an email account associated with said <u>actual</u> recipient e-mail address.

159.   (Currently amended) The method as in claim 155, wherein said access event comprises activation of an e-mail processing software associated with said <u>actual</u> recipient e-mail address.

160.   (Currently amended) The method as in claim 155, ~~further comprising the steps of:~~ <u>wherein the step of transmitting an e-mail from a sender computer includes attaching</u> ~~transmitting and delivering to the recipient e-mail address~~ an executable attachment file in conjunction with the e-mail ~~file~~, the executable attachment file having a first module for discovering the stored data <u>file</u> that is associated with said actual recipient's email address ~~, a second module for generating the confirmation of receipt notice, and a third module for transmitting the confirmation of receipt notice,~~

- 3 -

and upon the detection of the access event, automatically executing the first, second, and third modules of the executable attachment file and wherein the step of detecting an access event includes the step of executing the first module of the executable attachment file .

161.   (Currently Amended)   The method as in claim 160, wherein the executable attachment file has a fourth second module transmitted and delivered therewith, the fourth second module for detecting the access event, and

further comprising the step of:

automatically executing the fourth second module upon delivery of the attachment file to the actual recipient e-mail address.

162.   Canceled.

163.   (Currently amended)   The method as in claim 155, wherein said computer is a actual recipient email address is associated with a recipient computer.

164.   (Previously presented)   The method as in claim 163, wherein said recipient computer is a server of a service provider.

165.   (Currently amended)   The method as in claim 163, wherein said recipient computer is a user system that is directly accessible by the actual recipient, said user system including electronic mail processing software and being capable of receiving e-mail.

166.   (Currently amended)   The method as in claim 155, wherein said computer is a remote user computer may be used to from which said recipient may gain remote access to said actual recipient e-mail address.

- 4 -

167. (Currently amended) The method as in claim 155, wherein said <u>identifying data contained in said</u> stored ~~recipient~~ data <u>file</u> pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

168. (Currently amended) The method as in claim 155, wherein said stored ~~recipient~~ data <u>file</u> comprises ~~, at least in part,~~ identity information that identifies an individual.

169. (Previously presented) The method as in claim 168, wherein said identity information pertains to biometric identification.

170. (Currently amended) The method as in claim 169 further comprising ~~means for~~ <u>the step of</u> recognizing biometric attributes of an individual.

171. (Previously presented) The method as in claim 168, wherein said identity information includes alphanumeric text identification information.

172. (Currently amended) The method as in claim 155, wherein said stored ~~recipient~~ data <u>file</u> comprises ~~, at least in part,~~ information that identifies a business.

173. (Currently amended) The method as in claim 155, wherein said stored ~~recipient~~ data <u>file</u> comprises ~~, at least in part,~~ information that identifies an organization.

174. (Currently amended) The method as in claim 155, wherein said stored ~~recipient~~ data <u>file</u> comprises ~~, at least in part,~~ a computer generated user code.

175. (Currently amended) The method as in claim 155 further including the step of ~~including in said confirmation of receipt notice~~ <u>sending</u> access event data of ~~attendant~~ conditions <u>attendant of</u> said access event.

176. (Currently amended) The method as in claim 155, wherein said ~~party~~ <u>actual recipient</u> is an individual.

177. (Currently amended) The method as in claim 155, wherein said ~~party~~ <u>actual recipient</u> is a business.

178. (Currently amended) The method as in claim 155, wherein said ~~party~~ <u>actual recipient</u> is an organization.

179. (Currently amended) The method as in claim 155, wherein said ~~confirmation of receipt notice~~ <u>step of sending identifying data</u> is used to verify proper delivery of legal documents.

180. (Currently amended) The method as in claim 155, wherein said ~~confirmation of receipt notice~~ <u>step of sending identifying data</u> is used to verify proper delivery of confidential documents.

181. (Currently amended) The method as in claim 155, wherein said ~~recipient e-mail address~~ <u>data file</u> is ~~associated with a recipient~~ <u>stored on a</u> computer <u>associated with e-mail retrieval</u>.

182. (Currently amended) The method as in claim <u>155</u> ~~181~~, wherein said ~~recipient computer is a server of a service provider that is capable of receiving e-mail~~ <u>identifying data for confirming proper delivery of said e-mail is sent to an e-mail address</u>.

183.   Canceled.

184.   (Currently amended)   ~~A~~ The method ~~for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:~~ as recited in claim 258 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

~~a)   transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;~~

~~b)   delivering said e-mail to a recipient e-mail address;~~

~~c)   detecting an access event, and prompting the party who requested said access to enter recipient data prior to allowing the requested access, said recipient data identifying the party who requested said access;~~

~~d)~~ a) generating a confirmation of receipt notice wherein the ~~entered~~ inputted recipient data is included ~~in~~ with said confirmation of receipt notice; and

~~e)~~ b) sending said confirmation of receipt notice, wherein the ~~entered~~ inputted recipient data ~~contained in~~ included with said confirmation of receipt notice can be compared to ~~delivery~~ information associated with said intended recipient in order to verify whether the ~~email~~ e-mail was accessed by the intended recipient.

185.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

186.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said access event comprises access of an ~~email~~ e-mail account associated with said recipient e-mail address.

187. **(Currently amended)** The method as in claim ~~184~~ <u>236</u> , wherein said access event comprises activation of an e-mail processing software associated with said recipient e-mail address.

188. **(Currently amended)** The method as in claim ~~184~~ <u>236</u> , ~~further comprising the steps of:~~

~~transmitting and delivering to the recipient e-mail address~~ <u>wherein the step of transmitting an e-mail from a sender computer includes attaching</u> an executable attachment file in conjunction with the e-mail ~~file~~, the executable attachment file having a first module for prompting the party who requested said access event to enter recipient data~~, a second module for generating the confirmation of receipt notice, and a third module for transmitting the confirmation of receipt notice~~; and

~~upon the detection of the access event, automatically executing the first, second, and third modules~~ <u>and wherein the step of detecting an access event includes the step of executing the first module</u> of the executable attachment file.

189. **(Currently amended)** The method as in claim 188, wherein the executable attachment file has a ~~fourth~~ <u>second</u> module transmitted and delivered therewith, the ~~fourth~~ <u>second</u> module for detecting the access event, and further comprising the step of automatically executing the ~~fourth~~ <u>second</u> module upon delivery of the attachment file to the recipient e-mail address.

190. **Canceled.**

191. **(Currently amended)** The method as in claim ~~184~~ <u>236</u> , wherein said recipient e-mail address is associated with a recipient computer.

192. (Previously presented)   The method as in claim 191, wherein said recipient computer is a server of a service provider ~~that is capable of receiving e-mail~~ .

193. (Currently amended)   The method as in claim 191, wherein said recipient computer is a user system that is directly accessible by ~~the~~ a recipient, said user system including electronic mail processing software ~~and being capable of receiving e-mail~~ .

194. (Currently amended)   The method as in claim ~~184~~ 236 , wherein said ~~entered~~ inputted recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

195. (Currently amended)   The method as in claim ~~184~~ 236 , wherein said ~~entered~~ inputted recipient data comprises ~~, at least in part,~~ identity information that identifies an individual.

196. (Previously presented)   The method as in claim 195, wherein said identity information pertains to biometric identification.

197. (Currently amended)   The method as in claim 196 further comprising ~~means for~~ the step of recognizing biometric attributes of an individual.

198. (Previously presented)   The method as in claim 195, wherein said identity information includes alphanumeric text identification information.

199. (Currently amended)   The method as in claim ~~184~~ 236 , wherein said ~~entered~~ inputted recipient data comprises ~~, at least in part,~~ information that identifies a business.

- 9 -

200.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said ~~entered~~ inputted recipient data comprises ~~, at least in part,~~ information that identifies an organization.

201.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said ~~entered~~ inputted recipient data comprises ~~, at least in part,~~ a computer generated user code.

202.   (Currently amended)   The method as in claim ~~184~~ 236 further including the step of ~~including in said confirmation of receipt notice~~ sending access event data of attendant conditions of said access event.

203.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said ~~party~~ recipient is an individual.

204.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said ~~party~~ recipient is a business.

205.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said ~~party~~ recipient is an organization.

206.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said inputted recipient data ~~confirmation of receipt notice~~ is used to verify proper delivery of legal documents.

207.   (Currently amended)   The method as in claim ~~184~~ 236 , wherein said inputted recipient data ~~confirmation of receipt notice~~ is used to verify proper delivery of confidential documents.

- 10 -

208. (Currently amended) ~~A~~ The method recited by claim 260 ~~for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising~~ wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) ~~transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network~~ generating a confirmation of receipt notice wherein the acquired recipient data is included with said confirmation of receipt notice ; and

b) sending said confirmation of receipt notice, wherein the acquired recipient data contained with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient. ~~delivering said e-mail to a recipient e-mail address;~~

~~c) acquiring recipient data that is related to biometric identification of the recipient;~~

~~d) detecting an access event , and generating a confirmation of receipt notice wherein the acquired recipient data is included in said confirmation of receipt notice; and~~

~~e) sending said confirmation of receipt notice.~~

209. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

210. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said access event comprises access of an ~~email~~ e-mail account associated with said recipient e-mail address.

211. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said access event comprises activation of e-mail processing software associated with said recipient e-mail address.

- 11 -

212. (Currently amended) The method as in claim ~~208~~ 260 , ~~further comprising the step of:~~

~~transmitting and delivering to the recipient e-mail address~~ wherein the step of transmitting an e-mail from a sender computer includes attaching an executable attachment file in conjunction with the e-mail ~~file~~, the executable attachment file having a first module for acquiring recipient data that is related to biometric identification of the recipient, ~~a second module for generating the confirmation of receipt notice, and a third module for transmitting the confirmation of receipt notice;~~ and

~~upon the detection of the access event, automatically~~ wherein the step of detecting an access event includes the step of executing ~~at least~~ the ~~second and third modules~~ first module of the executable attachment file.

213. (Currently amended) The method as in claim 212, wherein the executable attachment file has a ~~fourth~~ second module transmitted and delivered therewith, the ~~fourth~~ second module for detecting the access event, and further comprising the step of:

automatically executing the ~~fourth~~ second module upon delivery of the attachment file to the recipient e-mail address.

214. Canceled.

215. (Currently amended) The method as in claim ~~208~~ 260 , wherein said recipient e-mail address is associated with a recipient computer.

- 12 -

216.   (Previously presented)   The method as in claim 215, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

217.   (Previously presented)   The method as in claim 215, wherein said recipient computer is a user system that is directly accessible by the recipient, said user system including electronic mail processing software and being capable of receiving e-mail.

218.   (Currently amended)   The method as in claim 208 260 , wherein said acquired recipient data is further related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

219.   (Currently amended)   The method as in claim 208 260 , wherein said acquired recipient data comprises identity information that identifies an individual.

220.   (Currently amended)   The method as in claim 208 260 further comprising means for recognizing biometric attributes of an individual.

221.   (Currently amended)   The method as in claim 208 260 , wherein said acquired recipient data comprises information that identifies a business.

222.   (Currently amended)   The method as in claim 208 260 , wherein said acquired recipient data comprises information that identifies an organization.

223.   (Currently amended)   The method as in claim 208 260 , wherein said acquired recipient data comprises a computer generated user code.

- 13 -

224. (Currently amended)   The method as in claim ~~208~~ 260 further including the step of ~~including in said confirmation of receipt notice~~ sending access event data of ~~attendant~~ conditions attendant ~~of~~ said access event.

225. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said recipient is an individual.

226. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said recipient is a business.

227. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said recipient is an organization.

228. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said ~~confirmation of receipt notice~~ sent recipient data is used to verify proper delivery of legal documents.

229. (Currently amended) The method as in claim ~~208~~ 260 , wherein said ~~confirmation of receipt notice~~ sent recipient data is used to verify proper delivery of confidential documents.

230. (Canceled).

231. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said recipient data is acquired as a requisite condition for permitting access to said delivered e-mail.

232. (Currently amended)   The method as in claim ~~208~~ 260 , wherein said recipient data is acquired as a requisite condition for permitting access to said recipient e-mail address.

- 14 -

233. (Currently amended) The method as in claim ~~208~~ 260 , wherein said recipient data is acquired as a requisite condition for operating a remote user computer, said remote user computer being operable to gain access to said recipient e-mail address.

234. (Currently amended) The method as in claim ~~208~~ 260 , wherein said recipient data is comprised of alphanumeric text, said alphanumeric text being associated with the at least one biometric attribute of said recipient.

235. (Currently amended) ~~A~~ The method as recited in claim 256 wherein the step of ~~for verifying whether an e-mail sent by a~~ sending at least some of the discovered identifying data for confirming proper delivery of said e-mail includes the steps of ~~party was accessed by an intended recipient, said method comprising~~ :

a) ~~storing recipient data on a computer associated with e-mail retrieval, said stored recipient data identifying a particular party;~~

~~b) transmitting an e-mail from a sender computer to the intended recipient, the sender computer being connected to a communications network;~~

~~c) delivering said e-mail to a recipient e-mail address;~~

~~d) detecting an access event, and discovering the stored recipient data that identifies the party associated with the recipient e-mail address to which such email was delivered;~~

~~e)~~ generating a confirmation of receipt notice wherein the acquired ~~the discovered recipient data~~ identifying data is included ~~in~~ with said confirmation of receipt notice; and

~~f)~~ b) sending said confirmation of receipt notice wherein the acquired identifying data contained with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient

.

- 15 -

236.   (Currently amended)   A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b) delivering said e-mail to a recipient e-mail address;

c) detecting an access event, and prompting the party associated with said access event to ~~enter~~ input recipient data prior to allowing the requested access, said recipient data including identifying data related to the party associated with said requested access; and

d) ~~generating a confirmation of receipt notice wherein the entered recipient data is included in said confirmation of receipt notice; and~~

~~e)~~ sending ~~said confirmation of receipt notice~~ recipient data for confirming proper delivery of said e-mail.

237.   (Currently amended)   ~~A~~ The method ~~for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising~~ recited by claim 264 wherein the step of sending data that identifies said recipient for confirming proper delivery of said e-mail includes the steps of :

a) generating a confirmation of receipt notice wherein the data that identifies the recipient is included with said confirmation of receipt notice ~~transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network~~; and

b) sending said confirmation of receipt notice, wherein the data that identifies the recipient that is included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient. ~~delivering said e-mail to a recipient e-mail address;~~

~~c) identifying said recipient via biometric identification;~~

- 16 -

d) detecting an access event, and generating a confirmation of receipt notice wherein data that identifies said recipient is included in said confirmation of receipt notice; and

e) sending said confirmation of receipt notice.

238. **(Currently amended)** The method as in claim ~~237~~ 264 , wherein said data that identifies said recipient is related to <u>a biometric imprint,</u> alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

239. **(Currently amended)** The method as in claim ~~237~~ 264 , wherein <u>the data that identifies</u> said recipient ~~data~~ is comprised of alphanumeric text, said alphanumeric text being associated with ~~the~~ at least one biometric attribute of said recipient.

240. **(Currently amended)** The method as in claim ~~237~~ 264 further <u>including the step of</u> ~~comprising means for~~ recognizing biometric attributes of an individual.

241. **(Currently amended)** The method as in claim ~~237~~ 264 , wherein said data that identifies said recipient comprises identity information that identifies an individual.

242. **(Currently amended)** The method as in claim ~~237~~ 264 , wherein said data that identifies said recipient comprises information that identifies a business.

243. **(Currently amended)** The method as in claim ~~237~~ 264 , wherein said data that identifies said recipient comprises information that identifies an organization.

244. **(Currently amended)** A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

- 17 -

a) a sender computer connected to a communications network and from which an email is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having <u>a</u> data storage ~~means~~ for storing said received e-mail;

c) ~~recipient~~ <u>a</u> data <u>file</u> stored on a computer associated with ~~the intended recipient~~ <u>e-mail retrieval</u> , said stored ~~recipient~~ data <u>file</u> associated with a particular recipient e-mail address and identifying a party associated with said particular e-mail address;

d) software capable of detecting an access event, wherein, upon detecting said access event, said software ~~executes the steps of:~~

    i. ~~retrieving~~ <u>discovers</u> the stored ~~recipient~~ data <u>file</u> that <u>is associated with the particular e-mail address to which said e-mail was delivered</u> ~~identifies the party associated with said particular recipient e-mail address to which such email was delivered~~ ; and

    ii. ~~including the acquired recipient stored data file in a confirmation of receipt notice; and~~

e) means for <u>sending the discovered data file for confirming proper delivery of said e-mail</u> ~~transmitting said confirmation of receipt notice to an e-mail address associated with said sending party~~ .

245. **(Currently amended)** The system as in claim ~~244~~ <u>275</u> , wherein said access event comprises access of a delivered e-mail.

246. **(Currently amended)** The system as in claim ~~244~~ <u>275</u> , wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

247.   (Currently amended)   The system as in claim ~~244~~ 275 , wherein said access event comprises activation of the e-mail processing software associated with the e-mail address to which said e-mail was delivered.

248.   (Currently amended)   A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having data storage means for storing said received e-mail;

c) software capable of detecting an access event, wherein, upon detecting said access event, said software ~~:~~

~~i.~~ prompts the party associated with said access event to ~~enter~~ input recipient data prior to allowing the requested access, ~~if no such recipient data pertaining to said party has been entered prior to said access event,~~ said recipient data comprising identifying data related to the party associated with said requested access; ~~and~~

~~ii.   includes the acquired recipient data in a confirmation of receipt notice;~~ and

~~e)~~ d)   means for sending recipient data for confirming proper delivery of said e-mail ~~transmitting said confirmation of receipt notice to an e-mail address associated with said sending party~~ .

249.   (Previously presented) The system as in claim 248, wherein said access event comprises access of a delivered e-mail.

250. (Previously presented) The system as in claim 248, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

251. (Currently amended) The system as in claim 248, wherein said access event comprises activation of ~~the~~ e-mail processing software associated with the e-mail address to which said e-mail was delivered.

252. (Currently amended) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer being capable of receiving said transmitted e-mail and further having data storage means for storing said received e-mail;

c) biometric identification means for recognizing biometric attributes of an individual;

d) software capable of detecting an access event <u>and identifying an individual through utilization of inputted biometric attributes of said individual</u> ~~, said software also being capable of acquiring biometric data identifying the party causing said access event, and including the acquired data in a confirmation of receipt notice~~ ; and

e) means for <u>sending data that identifies said individual for confirming proper delivery of said e-mail</u> ~~transmitting said confirmation of receipt notice to an e-mail address associated with said sending party~~ .

253. (Previously presented) The system as in claim 252, wherein said access event comprises access of a delivered e-mail.

- 20 -

254. **(Previously presented)**   The system as in claim 252, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

255. **(Currently amended)** The system as in claim 252, wherein said access event comprises activation of ~~the~~ e-mail processing software associated with the e-mail address to which said e-mail was delivered.

256. **(New)** A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data in a data file, said data file containing identifying data that identifies a recipient of e-mail and being associated with said recipient's e-mail address;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to an e-mail address;

d) detecting an access event, and discovering the stored data file that is associated with the e-mail address to which said e-mail was delivered; and

e) sending at least some of the identifying data contained in said discovered data file for confirming proper delivery of said e-mail.

257. (New) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data in a data file, said data file containing identifying data that identifies a recipient of e-mail and being associated with said recipient's e-mail address;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

- 21 -

c) delivering said e-mail to an e-mail address;

d) detecting an access event, and discovering the stored data file that is associated with the e-mail address to which said e-mail was delivered; and

e) sending the discovered data file for confirming proper delivery of said e-mail.

258.   (New) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b) delivering said e-mail to an e-mail address;

c) detecting an access event, and prompting the party that requested said access to input recipient data prior to allowing the requested access, said recipient data including identifying data that is associated with the party that requested said access; and

d) sending recipient data for confirming proper delivery of said e-mail.

259.   (New) The method recited by claim 236 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the inputted recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the inputted recipient data included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

260.   (New)   A method for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender

- 22 -

computer being connected to a communications network;

      b)   delivering said e-mail to a recipient e-mail address;

      c)   detecting an access event;

      d)   acquiring recipient data that is related to biometric identification of the recipient; and

      e)   sending recipient data for confirming proper delivery of said e-mail.

261.   **(New)** The method as recited in claim 260 wherein said recipient data is acquired prior to said access event.

262. (New) The method as recited in claim 260 wherein said recipient data is acquired after said access event.

263. (New) The method as recited in claim 260 wherein said recipient data is sent to an e-mail address.

264.   **(New)** A method for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

      a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

      b)   delivering said e-mail to an e-mail address;

      c)   identifying a recipient utilizing biometric identification;

      d) detecting an access event; and

      e)   sending data that identifies said recipient for confirming proper delivery of said e-mail.

265.   **(New)** The method as recited in claim 264 wherein said recipient is identified prior to said access event.

266. (New) The method as recited in claim 264 wherein said recipient is identified after said access event.

267. (New) The method as recited in claim 264 wherein said data that identifies said recipient is sent to an e-mail address.

268. (New) A method for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

    a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

    b) delivering said e-mail to an e-mail address;

    c) identifying a recipient in association with biometric identification;

    d) detecting an access event; and

    e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

269. **(New)** The method as in claim 268 wherein said recipient is identified prior to said access event

270. **(New)** The method as in claim 268 wherein said recipient is identified after said access event.

271. **(New)** The method as in claim 268 wherein said data that identifies said recipient is sent to an e-mail address.

272. (New) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

    a) storing recipient data on a storage element of a computer that is used by a recipient of e-mail to access e-mail, said recipient data including identifying data that is associated with a

- 24 -

recipient of e-mail;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to a recipient e-mail address;

d) detecting an access event and discovering at least part of said stored recipient data that is associated with said recipient;

e) sending at least part of said discovered recipient data for confirming proper delivery of said e-mail.

273. (New) The method recited in claim 272 wherein said recipient of e-mail is an actual recipient of said e-mail.

274. (New) The method recited in claim 244 wherein said recipient of e-mail is an actual recipient of said e-mail.

275. (New) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having a data storage for storing said received e-mail;

c) a data file stored on a computer, said stored data file containing identifying data pertaining to a party and associated with said party's e-mail address;

d) software capable of detecting an access event, wherein, upon detecting said access event, said software discovers identifying data contained in said stored data file that is associated with the e-mail address to which said e-mail was delivered; and

e) means for sending identifying data for confirming proper delivery of said e-mail.

276. (New)   The system as recited in claim 275 wherein said recipient of e-mail is an actual recipient of said e-mail.

277. (New)   The system as recited in claim 275 wherein said identifying data for confirming proper delivery of said e-mail is sent to an e-mail address.

278.   (New)   A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having a data storage for storing said received e-mail;

c) recipient data stored on the data storage of a computer that is used by a recipient of e-mail to access e-mail, said recipient data including identifying data that is associated with a recipient of e-mail;

d) software capable of detecting an access event, wherein, upon detecting said access event, said software discovers at least part of said stored recipient data that is associated with said recipient; and

e) means for sending at least part of said discovered recipient data for confirming proper delivery of said e-mail.

- 26 -

279. **(New)** The system as in claim 252, wherein said data that identifies said individual for confirming proper delivery of said e-mail is sent to an e-mail address.

280. **(New)** The system as recited in claim 278, wherein said recipient data is contained in a data file, said data file being stored on said storage of said computer.

281. **(New)** The system as recited in claim 278, wherein recipient data pertaining to said recipient of e-mail is stored on said storage prior to said access event.

282. **(New)** The system as recited in claim 278, wherein said at least part of said discovered recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

283. **(New)** The system as recited in claim 278, wherein said access event comprises access of a delivered e-mail.

284. **(New)** The system as recited in claim 278, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

285. **(New)** The system as recited in claim 278, wherein said access event comprises activation of an e-mail processing software associated with the e-mail address to which said e-mail was delivered.

286. **(New)** The method as recited in claim 257 wherein the step of sending the discovered data file for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the discovered data file is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the identifying data in the discovered data file that is included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

287. (New)   The method as recited in claim 272 wherein the step of sending at least part of said discovered recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the discovered recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the discovered recipient data included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

288. (New) The method as in claim 287, wherein said confirmation of receipt notice is sent to an e-mail address.

289.   (New) The method as in claim 272, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

290.   (New) The method as in claim 272, wherein said access event comprises access of an e-mail account associated with said recipient e-mail address.

291.   (New) The method as in claim 272, wherein said access event comprises activation of an e-mail processing software associated with said recipient e-mail address.

292. (New) The method as in claim 272, wherein the step of transmitting an e-mail from a sender computer includes attaching an executable attachment file in conjunction with the e-mail file, the executable attachment file having a first module for discovering the stored recipient data that is associated with said recipient, and wherein the step of detecting an access event includes the step of executing the first module of the executable attachment.

293. (New) The method as in claim 292, wherein the executable attachment file has a second module transmitted and delivered therewith, the second module for detecting the access event, and further comprising the step of:

automatically executing the second module upon delivery of the attachment file to said recipient e-mail address.

294. (New) The method as in claim 272, wherein said recipient e-mail address is associated with a recipient computer.

295. (New) The method as in claim 294, wherein said recipient computer is a server of a service provider.

296. (New) The method as in claim 294, wherein said recipient computer is a user system that is directly accessible by a recipient, said user system including electronic mail processing software.

297. (New) The method as in claim 272, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

298. (New) The method as in claim 272, wherein said computer on which said recipient data is stored is a recipient computer.

- 29 -

299. (New) The method as in claim 272, wherein said computer on which said recipient data is stored is a remote user computer.

300. (New) The method as in claim 272, wherein said recipient data is contained in a data file, said data file being stored on said storage element of said computer.

301. (New) The method as in claim 272, wherein said storage element comprises of a hard disk drive.

302. (New) The method as in claim 272, wherein said storage element comprises of a memory module.

303. (New) The method as in claim 272, wherein recipient data pertaining to said recipient of e-mail is stored on said storage element prior to said access event.

304.   (New) The method as in claim 272, wherein said stored recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

305.   (New) The method as in claim 272, wherein said stored recipient data comprises identity information that identifies an individual.

306.   (New) The method as in claim 305, wherein said identity information pertains to biometric identification.

307.   (New) The method as in claim 306 further comprising the step of recognizing biometric attributes of an individual.

308. (New) The method as in claim 305, wherein said identity information includes alphanumeric text identification data .

309. (New) The method as in claim 272, wherein said stored recipient data includes information that identifies a business.

310. (New) The method as in claim 272, wherein said stored data includes information that identifies an organization.

311. (New) The method as in claim 272, wherein said stored recipient data includes a computer generated user code.

312. (New) The method as in claim 272 further including the step of sending access event data of attendant conditions of said access event.

313. (New) The method as in claim 272, wherein said recipient is an individual.

314. (New) The method as in claim 272, wherein said recipient is a business.

315. (New) The method as in claim 272, wherein said recipient is an organization.

316. (New) The method as in claim 272, wherein said sent recipient data is used to verify proper delivery of legal documents.

317. (New) The method as in claim 272, wherein said sent recipient data is used to verify proper delivery of confidential documents.

318. **(New)**   The method as in claim 272, wherein said at least part of the discovered recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

319. **(New)**   The method as recited in claim 256, wherein said identifying data for confirming proper delivery of said e-mail is sent to an e-mail address.

320. **(New)** The method as recited in claim 256, wherein said data file is stored on a computer associated with e-mail retrieval.

321. **(New)**   The method as in claim 235, wherein said confirmation of receipt notice is sent to an e-mail address.

322.   **(New)** The method as in claim 256, wherein said identifying data contained in said stored data file pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

323. **(New)**   The method as in claim 257, wherein said data file is sent to an e-mail address.

324. **(New)**   The method as in claim 257, wherein said data file is stored on a computer associated with e-mail retrieval.

325. **(New)**   The method as in claim 286, wherein said confirmation of receipt notice is sent to an e-mail address.

326.   **(New)** The method as in claim 257, wherein said identifying data contained in said stored data file pertains to alphanumeric text identification, biometric identification, password

identification, a computer generated user code, or a combination thereof.

327. (New) The method as in claim 236, wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

328. (New) The method as in claim 236, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

329. (New) The method as in claim 236 wherein the party that is associated with said access event is an individual.

330. (New) The method as in claim 236 wherein the party that is associated with said access event is a business.

331. (New) The method as in claim 236 wherein the party that is associated with said access event is an organization.

332. (New) The method as in claim 258 wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

333. (New) The method as in claim 184, wherein said confirmation of receipt notice is sent to an e-mail address.

334. (New) The method as in claim 258, wherein said inputted recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

335. (New) The method as in claim 208, wherein said confirmation of receipt notice is sent to an e-mail address.

336. (New) The method as in claim 260, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

337. (New) The method as in claim 219, wherein said identity information includes alphanumeric text identification.

338. (New) The method as in claim 237, wherein said confirmation of receipt notice is sent to an e-mail address.

339. (New) The method as in claim 268 , wherein said data that identifies said recipient is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

340. (New) The method as in claim 268 further comprising the step of recognizing biometric attributes of an individual.

341. (New) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data on a storage element of a computer that is used to access e-mail, said recipient data including identifying data that is associated with a recipient of e-mail;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to an e-mail address;

d) detecting an access event and discovering at least part of said stored recipient data that is associated with said recipient;

e) sending at least part of said discovered recipient data for confirming proper delivery of said e-mail.

342. (New)   The system as in claim 244, wherein said discovered data file for confirming proper delivery of said e-mail is sent to an e-mail address.

343. (New)   The system as in claim 244, wherein said access event comprises access of a delivered e-mail.

344. (New)   The system as in claim 244, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

345. (New)   The system as in claim 244, wherein said access event comprises activation of an e-mail processing software associated with the e-mail address to which said e-mail was delivered.

346. (New)   The system as in claim 248, wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

347. (New)   The system as in claim 252, wherein said individual is identified prior to said access event.

348. (New)   The system as in claim 252, wherein said individual is identified after said access event.